UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/000,396	11/30/2001	John A. Copeland III	10775-36246	9056

7590 09/15/2005

John R. Harris
Morris, Manning & Martin, LLP
1600 Atlanta Financial Center
3343 Peachtree Rd. NE
Atlanta, GA 30326

EXAMINER	
BAUM, RONALD	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 09/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/000,396	**Applicant(s)** COPELAND, JOHN A.
	Examiner Ronald Baum	**Art Unit** 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6 and 8-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6 and 8-12* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *8/13/02, 5/19/03*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1- 6,8-12 are pending for examination.

2. Claims 1- 6,8-12 are rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1- 6,8-12 are rejected under 35 U.S.C. 102(b) as being anticipated by Shipley, U.S. Patent 6,119,236.

4. As per claim 1; "A method of analyzing network communication traffic for potential intrusion activity, comprising the steps of:

assigning packets to a flow [col. 3,lines 17-col. 12,line 35, whereas the "... dynamically detect patterns of behavior ...", "... automatically determining the configuration of the LAN...", etc., clearly encompasses the claimed limitations, insofar as for the determining /detection /comparison /control of the firewall to occur, that which is compared to the packet flow clearly must be defined /assigned, as broadly interpreted by the examiner.];

collecting flow data from packet headers [col. 3,lines 17-col. 12,line 35, whereas the "... dynamically detect patterns of behavior ...", "... automatically determining the configuration of the LAN...", etc., clearly encompasses the claimed limitations, insofar as for the determining /detection /comparison /control of the firewall to occur, the packet flow clearly must be collected per se, and such collection involves collection of the packets header data (i.e., the IP address, port, status flags, etc.,), as broadly interpreted by the examiner.];

analyzing collected flow data to assign a concern index value to the flow based upon a probability that the flow was not normal for data communications [col. 3,lines 17-col. 12,line 35, whereas the "… assign weight to breach…", and "… so as a weighted average might be used …" aspects of the post "… look for known patterns …", clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

maintaining an accumulated concern index from flows associated with a host; and

issuing an alarm signal once the accumulated concern index has exceeded an alarm threshold value [col. 3,lines 17-col. 12,line 35, whereas the "… assign weight to breach…", and "… react operation …" aspects of the post "… look for known patterns …", that involve the control and notification of the network associated firewall /gateway node, clearly encompasses the claimed limitations as broadly interpreted by the examiner.].".

5. Claim 2 ***additionally recites*** the limitation that; "The method of claim 1,

wherein the flow consists of the packets exchanged between two hosts that are associated with a single service.".

The teachings of Shipley suggest such limitations (col. 3,lines 17-col. 12,line 35, whereas the LAN and network aspects of the INSD interfaced to said network of multiple nodes, and the Internet /LAN port aspects insofar as port identification as relates to the Internet deals with port to port service designation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

6. Claim 3 ***additionally recites*** the limitation that; "The method of claim 1,

wherein the alarm signal updates a firewall for filtering packets transmitted by a host. ". The teachings of Shipley suggest such limitations (col. 3,lines 17-col. 12,line 35, whereas the "... assign weight to breach...", and "... react operation ..." aspects of the post "... look for known patterns ...", that involve the control and notification of the network associated firewall /gateway node, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

7. Claim 4 ***additionally recites*** the limitation that; "The method of claim 1,

wherein the alarm signal generates a notification to the network administrator.". The teachings of Shipley suggest such limitations (col. 3,lines 17-col. 12,line 35, whereas the "... assign weight to breach...", and "... react operation ..." aspects of the post "... look for known patterns ...", that involve the control and notification of the network associated firewall /gateway node and subsequent "... network administrator has time to evaluate ...", clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

8. Claim 5 ***additionally recites*** the limitation that; "The method of claim 1,

wherein each concern index value associated with a respective potential intrusion activity is a predetermined fixed value.".

The teachings of Shipley suggest such limitations (col. 3,lines 17-col. 12,line 35, whereas the "... assign weight to breach...", and "... so as a weighted average might be used ..." aspects of the post "… look for known patterns …", clearly encompasses the claimed limitations, insofar as an average is a "predetermined fixed value", as broadly interpreted by the examiner.).

9. As per claim 6; "A method of analyzing network communication traffic for potential intrusion activity, comprising the steps of:

assigning packets to a flow

wherein a flow consists of the packets exchanged between two hosts that are associated with a single service [col. 3,lines 17-col. 12,line 35, whereas the LAN and network aspects of the INSD interfaced to said network of multiple nodes, and the Internet /LAN port aspects insofar as port identification as relates to the Internet deals with port to port service designation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

collecting flow data from packet headers [col. 3,lines 17-col. 12,line 35, whereas the "… dynamically detect patterns of behavior …", "… automatically determining the configuration of the LAN…", etc., clearly encompasses the claimed limitations, insofar as for the determining /detection /comparison /control of the firewall to occur, the packet flow clearly must be collected per se, and such collection involves collection of the packets header data (i.e., the IP address, port, status flags, etc.,), as broadly interpreted by the examiner.];

analyzing collected flow data to assign a concern index value

wherein each concern index value associated with a respective potential intrusion activity is a predetermined fixed value [col. 3,lines 17-col. 12,line 35, whereas the "… assign weight to breach…", and "… so as a weighted average might be used …" aspects of the post "... look for known patterns ...", clearly encompasses the claimed limitations, insofar as an average is a "predetermined fixed value", as broadly interpreted by the examiner.];

maintaining an accumulated concern index from flows associated with a host; and

issuing an alarm signal once the accumulated concern index has exceeded an alarm threshold value [col. 3,lines 17-col. 12,line 35, whereas the "... assign weight to breach...", and "... react operation ..." aspects of the post "... look for known patterns ...", that involve the control and notification of the network associated firewall /gateway node, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]."

10. As per claim 8; "A method of analyzing network communication traffic for potential intrusion activity, comprising the steps of:

assigning packets to a flow

wherein a flow consists of the packets exchanged between two Internet Protocol addresses with at least one port remains constant [col. 3,lines 17-col. 12,line 35, whereas the LAN and network aspects of the INSD interfaced to said network of multiple nodes, and the Internet /LAN port aspects insofar as port identification as relates to the Internet deals with port to port service designation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

collecting flow data from packet headers [col. 3,lines 17-col. 12,line 35, whereas the "... dynamically detect patterns of behavior ...", "... automatically determining the configuration of the LAN...", etc., clearly encompasses the claimed limitations, insofar as for the determining

/detection /comparison /control of the firewall to occur, the packet flow clearly must be collected per se, and such collection involves collection of the packets header data (i.e., the IP address, port, status flags, etc.,), as broadly interpreted by the examiner.];

analyzing collected flow data to assign a concern index value to the flow [col. 3,lines 17-col. 12,line 35, whereas the "... assign weight to breach...", and "... so as a weighted average might be used ..." aspects of the post "... look for known patterns ...", clearly encompasses the claimed limitations, insofar as an average is a "predetermined fixed value", as broadly interpreted by the examiner.];

maintaining a host structure containing an accumulated concern index from flows associated with the host; and

issuing an alarm once the accumulated concern index has exceeded an alarm threshold value [col. 3,lines 17-col. 12,line 35, whereas the "... assign weight to breach...", and "... react operation ..." aspects of the post "... look for known patterns ...", that involve the control and notification of the network associated firewall /gateway node, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]."

11. Claim 9 ***additionally recites*** the limitation that; "The method of claim 8,

wherein each concern index value associated with a respective potential intrusion activity is a predetermined fixed value.".

The teachings of Shipley suggest such limitations (col. 3,lines 17-col. 12,line 35, whereas the "... assign weight to breach...", and "... so as a weighted average might be used ..." aspects of the post "... look for known patterns ...", clearly encompasses the claimed limitations, insofar as an average is a "predetermined fixed value", as broadly interpreted by the examiner.).

12. As per claim 10, this claim is the apparatus/system for the method claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection; "A system for analyzing network communication traffic, comprising:

a computer system operable to

classify packets into flows,

collect flow data from packet header information,

analyze collected flow data to assign a concern index value

wherein each concern index value associated with a respective potential intrusion activity is a predetermined fixed value, and

generate an alarm signal; and

a communication system coupled to the computer system operable to

send packets from one host to another host."

13. As per claim 11, this claim is the apparatus/system for the node processor element with associated database element for the method claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection; "A system for analyzing network communication traffic, comprising:

a processor operable to

classify packets into flows,

collect flow data from packet header information,

analyze collected flow data to assign a concern index value

wherein each concern index value associated with a respective potential intrusion activity is a predetermined fixed value, and

generate an alarm signal;

memory coupled to the processor operable to store the flow data;

a database coupled to processor operable to

store log files; and

a network interface coupled to the processor operable to

monitor network traffic."

14. As per claim 12, this claim is a specific attack method for claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; "A method of analyzing network communication traffic for potential intrusion activity, comprising the steps of:

analyzing packet header information;

determining a transport level protocol specifying a format of a data area [col. 3,lines 17-col. 12,line 35, generally, and col. 6,lines 31-67 more specifically, whereas the "... access ports that do not exist ...", and "... the multitude of responces (such as synchronization requests) forthcoming through the internet ..." aspects of "...determining a transport level protocol ...", that involves the DOS type attack (i.e., SYN flooding use of minimal byte data field, at the transport layer), clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

issuing an alarm when

the transport level protocol is identified as User Datagram Protocol and

the data segment associated with User Datagram Protocol packet contains

two or

less bytes of data [col. 3,lines 17-col. 12,line 35, whereas the "… assign weight to breach…", and "… react operation …" aspects of the post "… issuing an alarm … transport level protocol … User Datagram Protocol packet contains …", that involve the control and notification of the network associated firewall /gateway node, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]."

Conclusion

15. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum
Patent Examiner

Primary Examiner
AU 2131
9/9/05